IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BRITISH TELECOMMUNICATIONS PLC and BT AMERICAS, INC.,	)	
Plaintiffs,	)	C.A. No. 22-01538-CJB
V.	)	**JURY TRIAL DEMANDED**
PALO ALTO NETWORKS, INC.,	)	
Defendant.	)	

PLAINTIFFS' OPPOSITION TO DEFENDANT'S
MOTION TO DISMISS UNDER RULE 12(b)(6)

OF COUNSEL:

Bart H. Williams
PROSKAUER ROSE LLP
2029 Century Park East
Suite 2400
Los Angeles, California 90067
310-557-2900
bwilliams@proskauer.com

Baldassare Vinti
Nolan M. Goldberg
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
212-969-3000
bvinti@proskauer.com
ngoldberg@proskauer.com

Edward Wang
PROSKAUER ROSE LLP
1001 Pennsylvania Avenue NW
Suite 600
Washington, DC 20004
202-416-6800
ewang@proskauer.com

Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
POTTER ANDERSON & CORROON LLP
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

Attorneys for Plaintiff British Telecommunications plc and BT Americas, Inc.

Dated: March 20, 2023

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. NATURE AND STAGE OF PROCEEDINGS 7

III. BACKGROUND 7

A. BT's Complaint 7

1. Limitations of Prior Art Cybersecurity Methods. 8

2. The Patents Revolutionized the Field of Cybersecurity. 8

B. The Cybersecurity Industry, Including PAN, Has Broadly Adopted the Claimed Inventions and Touted Their Advantages. 12

IV. ARGUMENT 13

A. PAN's Motion Improperly Rests on Disputing Material Facts. 13

B. The Claims are Not Directed to An Abstract Idea; They Are Directed to Improvements in Computer Functionality By Way of a Novel Architecture 15

C. The Claims Contain Inventive Concepts Sufficient to Transform any Alleged Abstract Idea into Patent Eligible Subject Matter. 19

V. CONCLUSION 20

TABLE OF AUTHORITIES

Page(s)

CASES

Aatrix Software, Inc. v. Green Shades Software, Inc.,
882 F.3d 1121 (Fed. Cir. 2018).....16

Affinity Labs of Tex., LLC v. DIRECTV, LLC,
838 F.3d 1253 (Fed. Cir. 2016).....16, 20

Alice Corp. v. CLS Bank International,
573 U.S. 208 (2014).....13, 20

Ancora Techs., Inc. v. HTC Am., Inc.,
908 F.3d 1343 (Fed. Cir. 2018), *as amended* (Nov. 20, 2018).....17

Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC,
827 F.3d 1341 (Fed. Cir. 2016).....15, 18

Berkheimer v. HP Inc.,
881 F.3d 1360 (Fed. Cir. 2018).....19

CardioNet, LLC v. InfoBionic, Inc.,
955 F.3d 1358 (Fed. Cir. 2020).....17

Cellspin Soft, Inc. v. Fitbit, Inc.,
927 F.3d 1306 (Fed. Cir. 2019).....15

Content Extraction & Transmission LLC v. Wells Fargo Bank Nat'l Ass'n,
776 F.3d 1343 (Fed. Cir. 2014).....18

Coop. Ent., Inc. v. Kollective Tech., Inc.,
50 F.4th 127 (Fed. Cir. 2022) ..... *passim*

Doe v. Princeton Univ.,
790 F. App'x 379 (3d Cir. 2019) 12

Elec. Power Grp., LLC v. Alstom S.A.,
830 F.3d 1350 (Fed. Cir. 2016).....18

Enfish, LLC v. Microsoft Corp.,
822 F.3d 1327 (Fed. Cir. 2016).....17

F45 Training Pty Ltd. v. Body Fit Training USA Inc.,
No. 20-cv-1194, 2021 WL 2779130 (D. Del. July 2, 2021).....15

Finjan, Inc. v. Blue Coat Sys., Inc.,
879 F.3d 1299 (Fed. Cir. 2018).....20

Genedics, LLC v. Meta Co.,
No. 17-cv-1062, 2018 WL 3991474 (D. Del. Aug. 21, 2018).....14

Gracenote, Inc. v. Free Stream Media Corp.,
No. 18-cv-1608, 2019 WL 6728450 (D. Del. Dec. 11, 2019) 18

IBM Corp. v. Zillow Grp., Inc.,
50 F.4th 1371 (Fed. Cir. 2022) 18

ICON Health & Fitness, Inc. v. Polar Electro Oy,
243 F. Supp. 3d 1229 (D. Utah 2017),
aff'd, 717 F. App'x 1005 (Fed. Cir. 2018)..... 18-19

In re Rosenberg,
813 F. App'x 594 (Fed. Cir. 2020) 18

MAZ Encryption Techs. LLC v. Blackberry Corp.,
No. 13-cv-304, 2016 WL 5661981 (D. Del. Sept. 29, 2016).....14

Mgmt. Sci. Assocs., Inc. v. Datavant, Inc.,
510 F. Supp. 3d 238 (D. Del. 2020).....1

RICPI Commc'ns LLC v. JPS Interoperability Sols., Inc.,
No. 18-cv-1507, 2019 WL 1244077 (D. Del. Mar. 18, 2019).....15

S.I.SV.EL. Societa Italiana per lo Sviluppo Dell'Elettronica S.P.A v. Rhapsody Int'l Inc.,
No. 18-cv-69, 2019 WL 2298795 (D. Del. May 30, 2019) 13

SAP Am., Inc. v. InvestPic, LLC,
898 F.3d 1161 (Fed. Cir. 2018).....13, 18

SRI International, Inc. v. Cisco Systems, Inc.,
930 F.3d 1295 (Fed. Cir. 2019)..... *passim*

TecSec, Inc. v. Adobe Inc.,
978 F.3d 1278 (Fed. Cir. 2020).....17

Thales Visionix Inc. v. United States,
850 F.3d 1343 (Fed. Cir. 2017).....18

TMI Sols. LLC v. Bath & Body Works Direct, Inc.,
No. 17-cv-965, 2018 WL 4660370 (D. Del. Sept. 28, 2018).....19

Twilio, Inc. v. Telesign Corp.,
249 F. Supp. 3d 1123 (N.D. Cal. 2017) 16, 18, 19

WSOU Invs., LLC v. Netgear, Inc.,
No. 21-cv-1119, 2022 WL 2753005 (D. Del. July 14, 2022),
report and recommendation adopted, No. 21-cv-1119, 2022 WL 3017109 (D. Del. July 29, 2022).....14

Xpoint Techs., Inc. v. Microsoft Corp.,
730 F. Supp. 2d 349 (D. Del. 2010).....7

I. INTRODUCTION

Plaintiffs British Telecommunications PLC and BT Americas, Inc. (collectively, "BT") oppose the motion to dismiss by Defendant Palo Alto Networks, Inc. ("PAN") alleging invalidity of U.S. Patent Nos. 7,159,237 ("'237 Patent") (Complaint ("Compl.") Ex. A, D.I. 1.01) and 7,895,641 ("'641 Patent") (Compl. Ex. B, D.I. 1.01) (collectively, "the Patents") under 35 U.S.C. § 101 (D.I. 12) ("PAN's Motion" or "Mot.").

BT's well-pleaded factual allegations demonstrating the subject matter eligibility of the Patents' claims are pulled straight from the intrinsic record (Compl. ¶¶ 11-39, D.I. 1) and must be treated as true. *Mgmt. Sci. Assocs., Inc. v. Datavant, Inc.*, 510 F. Supp. 3d 238, 244 (D. Del. 2020). The Patents claim a specific, multi-tier structural computer and network architecture that improves a performance of devices that secure computer networks as well as improves the performance of the network of such devices through cross-device correlation. Compl. ¶ 16. This is not a self-serving statement in a complaint; the Patents expressly call out the invention, for example, as "*render[ing] more effective*, a customer's existing preventive security products." '237 Patent at 1:60-62 (emphasis added). As in *SRI International, Inc. v. Cisco Systems, Inc.*, 930 F.3d 1295, 1303 (Fed. Cir. 2019), the claimed architecture comprises a non-conventional and non-generic arrangement (*i.e.*, computer architecture) "necessarily rooted in computer technology in order to solve a specific problem in the realm of computer networks"—here, the detection of previously unknown attacks or security events in computer networks in an efficient and accurate manner and also in a way that can be delivered as a "managed . . . service," where providers like PAN can continually optimize the security devices of multiple customers. *See* '237 Patent at 1:49-52.

Over two decades ago, Dr. Bruce Schneier, a world-renowned cybersecurity expert, along with his co-inventors, leading scientists themselves, invented the claimed architecture after recognizing that existing security solutions generally tried to prevent *known* viruses from

infiltrating computer systems. Compl. ¶¶ 31-37. Dr. Schneier and his co-inventors solved for the many competing constraints that must be balanced for a security solution to succeed in detecting and preventing *unknown* threats, including, for example, the: (1) surplus of information that needs to be considered to find unknown security threats ('237 Patent at 1:62-67); (2) capacity and expertise limitations of a customer's security personnel (*id.* at 1:25-28); (3) false positives, where legitimate traffic is designated as malicious thereby impeding the operation of the network (*id*. at 2:3-8); and (4) need to rapidly refine the security solution to be effective (*id*. at 2:30-32). The novel architecture claimed in the Patents addressed the problems of the prior art and the technical constraints that limited solutions to those problems at the time of the invention.

PAN ignores, and at other times disputes, the Complaint's factual allegations. PAN tries to recast the invention as directed to an abstract idea of simply collecting, filtering, and analyzing data, and then transmitting information about that data to a human for feedback. PAN also tries to reduce the invention to a process that humans could perform. But that is not the invention the Patents claim. PAN deliberately ignores the Patents' tiered hierarchical architecture with defined structure and a defined series of steps that must be followed to achieve the desired results. *See infra* III.A.2. To this end, the Patents do not cover all systems that simply collect, filter, analyze and transmit data regardless of specific structure or architecture. How the elements are arranged and structured matters. And here, it is precisely the invention's organization and structure that improved the performance of network security devices and revolutionized the industry.

For example, PAN argues that "[t]he Claims invoke generic computing components to . . . filter[] . . . data." Mot. at 1. But, PAN ignores that the claims require positive and negative filtering

of a specific subset of network traffic identified as "status data" at a probe.[1] In other words, the claims do not cover abstract filtering, but rather the use of two different types of filters (positive and negative) applied to specific data (status data) at a specific location (the probe).

PAN similarly argues that "[t]he Claims invoke generic computing components to . . . analyz[e] data." Mot. at 1. Again, a gross over-simplification. First, the invention analyzes the data that would previously have been discarded (*i.e.*, residue), an analysis specific to the invention of the Patents. Indeed, the United States Patent and Trademark Office ("USPTO") noted during prosecution that in the prior art "all data is filtered by intrusion detection, firewall, gateway, proxy, sensor, probe, or sentry, or some other type of device" such that "if an attack occurs the data is transmitted for further analysis" but ***"[a]ll other data is usually blocked or discarded."*** Compl. ¶ 38. (alteration in original) (emphasis added) (quoting Notice of Allowability at 4). The Patents disclose a different system that does not need to wait for an attack to happen before the residue is mined so as to prevent that attack from happening in the first place.

Second the invention looks at residue not once, but twice, for two different purposes, and in two different locations. First, the invention analyzes the residue to detect possible events at a first level in a network hierarchy. *See*, *e.g.*, '641 Patent, Claim 1 ("a filtering subsystem coupled to analyze . . . ."). Then, the invention sends information relating to these possible threats to a higher hierarchical level that can more effectively determine whether the "possible event" is an actual event or a false positive. *See*, *e.g.*, *id*., Claim 1 ("a communications system coupled to

[1] Indeed, Judge Connolly adopted a claim construction of residue to be "status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering." Ex. 3, *Brit. Telecomms. Plc & BT Ams., Inc. v. Fortinet, Inc.*, No. 18-cv-01018 (D. Del., filed July 10, 2018), D.I. 157 at 4.

transmit information about the identified events to an analyst system . . . ."). This two-level review balances competing constraints and results in optimal detection.

PAN argues that "[t]he Claims invoke generic computing components to . . . transmit[] information about that data to a human for feedback," and that the claims are directed to simply sending "data to a human for feedback." Mot. at 1. But PAN ignores that the tiered analysis that precedes the transmittal to the analyst (positive and negative filtering, followed by a first analysis of residue for potential events) materially reduces the burden on the secure operations center ("SOC") by reducing the amount of data that needs to be transmitted to it, and thus freeing up the analysts to focus on what matters. As the Patents explain, "An effective monitoring, detection and response system should be designed not to replace a customer's system administrators but to augment their abilities." '237 Patent at 1:23-25. Further, PAN ignores the presence and impact of the feedback loop itself. *Id*. at 3:51-53 ("This continuous improvement allows the invention to take full advantage of . . . the monitoring system.").

PAN also ignores that the specific tiered hierarchical architecture claimed artfully balances between accuracy and speed to solve the technological problems arising in traditional security systems. For example, while the use of a feedback loop at the probe (where detections made based on the residue are fed back into the lower level of the hierarchy to improve its operation over time) would make the system faster, it would be less accurate because it would lack the confirmation at the second stage of the hierarchy that the detection actually poses a threat (i.e., more likely to be a false positive) whereas feedback from the SOC is slower, but more accurate. Similarly, while forwarding all traffic (and not just certain data) to the SOC improves accuracy, such a design would have time and capacity constraints. The tiered

architecture specifically claimed in the Patents realizes these benefits while minimizing or eliminating the burdens associated with traditional, generic systems.

The architecture also creates a system where cross-probe correlation can occur. Prior art systems typically consisted of software placed at a single point in the network (*e.g.,* at the edge) and therefore lacked the necessary architecture for cross-probe correlation. And while it is the architecture of the independent claims that enables this benefit, certain dependent claims also explicitly recite this improvement to computer security systems. *See*, *e.g.*, *id*., Claim 14; '641 Patent, Claim 14. Notably, "cross-probe correlation" does not refer to any "probe," but specifically the probes described by the independent claims.[2] Therefore, the correlation of these probes are tied to the claimed filtering and analysis performed by these probes, from which the information is then transmitted up the claimed hierarchy to a SOC for cross-probe correlation. These probes can then receive feedback (as claimed) based on this cross-probe correlation and improve the overall functioning of this computer security technology like never before (at the time of the invention). In other words, the invention not only improves the performance of each probe over time, but also the performance of all probes that connect to the same SOC.

While all of this may seem conventional today, more than 20 years after the conception of this invention, it did not exist previously and, as Dr. Schneier explained, revolutionized the security industry. The Patents' architectural solution, which is expressly reflected in the asserted independent claims, and illustrated in Figure 1, is not abstract because it is a technological solution to improve upon existing network security products. *See* '237 Patent at 3:60-61 ("FIG.

[2] Chief Judge Connolly adopted a construction of "Probe" to mean "a component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis." Ex. 3 at 2.

1 is an overview of the *system architecture* of an exemplary embodiment of the present invention" (emphasis added)); *see also id*. at 1:60-65 (noting MSM service meant "to supplement, and thereby render more effective, a customer's existing preventive security products.").

Outside of litigation, PAN repeatedly touts the benefits of the architecture claimed in the Patents as reasons why customers should buy its infringing devices. *See infra* Section III.B. Yet PAN's Motion is predicated on disputing these facts (and others) in the Complaint. This is grounds alone to reject PAN's Motion because the Court must accept BT's well-pleaded facts as true and draw "all reasonable inferences from the intrinsic and Rule 12 record in favor of the non-movant." *Coop. Ent., Inc. v. Kollective Tech., Inc.*, 50 F.4th 127, 130 (Fed. Cir. 2022) (collecting cases) (discussing patent eligibility under 101 at Rule 12 stage).

PAN's Motion also fails on even more grounds. For example, PAN's analysis of *Alice* step one does not address the improvement of the entirety of the claimed inventions over the prior art. Instead, PAN merely argues discrete elements of the claims, such as "filtering data", are abstract. But the Patents are directed to an architecture incorporating these elements in specific ways to improve the computer network.

As to *Alice* step two, PAN again zooms in on certain individual elements in isolation and argues they are not inventive (and, of course, the Patents never claimed they were), while ignoring the inventive tiered analysis of the residual data which the USPTO found to be a novel step. Moreover, PAN ignores the inventive improvements in computer technology—in this case security solutions provided by the claims as a whole. PAN's arguments run contrary to the established law that "useful improvements to computer networks are patentable regardless of whether the network is comprised of standard computing equipment." *Coop.*, 50 F.4th at 135.

For these reasons and those below, PAN's Motion should be denied.

II. NATURE AND STAGE OF PROCEEDINGS

Chief Judge Connolly who initially presided over this case also presided over a related case involving the Patents. *See* Ex. 3[3]. This case was then referred to Your Honor with consent of the parties. D.I. 10. On February 2, 2023, PAN moved to dismiss the Complaint (D.I. 11) and transfer the case to the Northern District of California (D.I. 13).

III. BACKGROUND

A. BT's Complaint

BT alleges that numerous PAN products infringe each of the Patents, including each of the independent claims and at least certain of the dependent claims.[4] *See, e.g.*, Compl. ¶ 41. The independent claims of the Patents reflect the inventive architecture exemplified in Figure 1 of the Patents, where, for example, the effectiveness of pre-existing security products, such as Firewall 1010, is improved by connecting them to a larger system, which includes Probe 2000, PIPES 3000, and SOCRATES Problem and Expertise Management System 6000 at a SOC. Far from being an abstract concept, the claims recite specific activities that are supposed to happen at specific locations and in a specific sequence.

This action follows a patent infringement suit BT filed against Fortinet in this Court involving the Patents. After Judge Connolly issued a *Markman* order, which BT viewed as extremely favorable to its case, the parties settled. The Patents also each withstood Fortinet's

[3] Cites to "Ex." refer to the exhibits to the Declaration of Edward Wang.

[4] The '237 Patent consists of 42 claims, 3 of which are independent (claims 1, 18, and 26). The '641 Patent contains 25 claims, 2 of which are independent (claims 1 and 18). The arguments below apply with equal force to every claim addressed by PAN, but some additional arguments below are applicable only to certain claims. At this stage, BT is "not required to . . . identify which claims it is asserting." *Xpoint Techs., Inc. v. Microsoft Corp.*, 730 F. Supp. 2d 349, 353 (D. Del. 2010).

inter-partes review challenges at the Patent Trial and Appeal Board ("PTAB") where the PTAB declined to institute review proceedings based on the weakness of that cited art. *See* Ex. 1, *Fortinet Inc. v. BT Ams., Inc.*, IPR2019-01324, Paper 9; Ex. 2, *Fortinet Inc. v. BT Ams., Inc.*, IPR2019-01325, Paper 9.[5]

1. Limitations of Prior Art Cybersecurity Methods.

Invented by world-renowned cybersecurity expert Dr. Bruce Schneier[6] and his two co-inventor colleagues, the Patents' claims fundamentally improved upon the functionality of prior cybersecurity systems, by (among other advantages) allowing for the detection of previously unknown attacks or security events. Compl. ¶¶ 16, 34. For example, prior art solutions were limited in their ability to detect and address previously unknown threats quickly enough to prevent often catastrophic damage to a computer system. *Id.* ¶ 36. Indeed, "[w]hile automatic defenses may work against automated attacks, they are at a disadvantage against an intelligent attack, against which is needed the kind of intelligent defense offered by" the Patents. '237 Patent at 1:40-43. As explained, in the next section, the invention of the Patents not only improved upon the prior art solutions, it revolutionized the field of cybersecurity.

2. The Patents Revolutionized the Field of Cybersecurity.

The novel security architecture claimed in the Patents "spawned an entirely new product category—called Managed Security Monitoring [("MSM")]—which has since come to be a very

[5] The Complaint incorporates pertinent details from the intrinsic record, including facts submitted to the PTAB via a sworn statement of Dr. Schneier. *See, e.g.*, Compl. ¶¶ 11-39; Compl. Ex. C, D.I. 1.01.

[6] Dr. Schneier, called a "security guru" by the *Economist*, teaches computer security and cryptography at Harvard's Kennedy School of Government, has written multiple books on this subject, including a definitive book on cryptography, has testified before Congress numerous times, published hundreds of articles, holds dozens of patents, and hosts a widely followed cybersecurity blog. Compl. ¶ 30. Dr. Schneier is sufficiently famous that he rated mention in the De Vinci Code—and is often called the "Chuck Norris of Security." *Id.*

large commercial space." Compl. Ex. C. ¶ 3. The Patents teach that MSM "is not intended to replace but to supplement, and thereby render more effective, a customer's existing preventive security products." '237 Patent at 1:60-62. These products allowed coordination of information from both the customer site and third parties, like PAN (and other customer sites through cross-probe correlation), who could provide more analysis of potentially unknown attacks and improve the effectiveness of pre-existing security devices, such as firewalls. *See, e.g.*, *id*., Claim 18.

The claimed architecture provides novel systems for dynamically responding to and protecting against new and constantly evolving malware and potential network attacks while simultaneously generating fewer false positive alerts that could strain resources and impede a computer network's performance. Compl. ¶¶ 37-38. The architecture achieves these results through an innovative tiered structure that more effectively weeds out known security threats and benign traffic (through filtering related status data), to locate and analyze residual (or otherwise uncategorized) status data that may be malicious (including threats never seen before), then confirming whether the data is actually malicious, using a two tiered process that balances accuracy with efficiency, and then update the system with the results of the analysis. *Id.*

The architecture begins by collecting "status data"—that is, "data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components"—via a probe or sensor at the security monitoring system. Ex. 3 at 1.[7] The probe then filters the status data to determine whether it corresponds to information that is already known and categorized, such as existing security threats or known legitimate traffic. Compl. ¶ 37.

[7] PAN's argument that the claimed inventions are directed to amorphous "data" (Mot. at 3) is factually incorrect and contradicted by the construction adopted in this District's claim construction order for the term "status data," which is the particular type of network data provided in quotes. *See* Ex. 3 at 1.

Prior art systems would stop there and discard any remaining uncategorized data—the residual status data. *See id*. ¶¶ 36-37. Indeed, the patent examiner acknowledged this particular advance over the prior art, stating that in the prior art, "all data is filtered by intrusion detection, firewall, gateway, proxy, sensor, probe, or sentry, or some other type of device" such that "if an attack occurs the data is transmitted for further analysis" but ***"[a]ll other data is usually blocked or discarded."*** *Id*. ¶ 38. (alteration in original) (emphasis added) (quoting Notice of Allowability, at 4). The inventions claimed by the Patents, in contrast, do not discard the residual status data, but further analyze it; first at the probe, which makes an initial assessment as to whether the residual status data reflects a possible malicious event. *Id.* ¶ 37; '237 Patent, Claim 1(c).

But the claimed architecture does not stop its analysis of residual status data at the probe. It then transmits the potential security events identified by the probe to a SOC for further analysis by analysts or analyst systems (depending on the claim in question), which are best equipped to analyze this narrower set of data because they have access to broader information to determine whether the potential event is an actual event or a false positive. Compl. ¶ 37; *see also* '237 Patent, Claim 1. The analyst or analyst system further provides feedback to the probes, without the need to go offline, which improves the overall system's security capabilities over time. *Id*.

The Patents' inventive aspects are tied directly to the claims. It is the claimed series of steps—taken by specific components within the claimed structural architecture with a specific sequence—that ultimately allows the system to not only detect new, unknown, and evolving attacks, but also dynamically respond to and continually improve the system's ability to detect those threats, all while maximizing system performance and efficiency. *See id.* ¶¶ 16, 37-38. The claims' specific combination and sequence of elements reflect the novel architecture the inventors

created to improve "network security" and enable "dynamic network intrusion monitoring, detection, and response." '237 Patent at 1:7-9.

Indeed, an inventive feature of the claims is that the architecture maximizes the network's limited resources where they are most needed, allowing the system to be scaled without compromising network performance or limiting detection capabilities. Whereas the probe (which includes, among other things, information about known security events) is well equipped to analyze large amounts of data, it has access to less information, and is thus more likely to generate a false positive. *Id.* at 3:15-19. Were the system to rely solely on the probe to make decisions about novel security events, it could mischaracterize benign data as a threat or mischaracterize a threat as benign data—clearly an undesirable and unacceptable result that would degrade the functionality of the network and the security system. *See, e.g.*, *id.* at 2:3-8. Moreover, whereas the analyst or analyst systems at the SOC are well equipped to determine whether residual status data is benign or constitutes a threat because of the broader access to information (including, for certain dependent claims, information from multiple probes), they are poorly equipped to process large amounts of data. *Id.* at 1:60-2:8. While the claimed architecture is now common-place, it was unintuitive at the time the inventors filed the Patents. It is this unconventional combination of steps in the claimed architecture—including analyzing residual status data at two different hierarchical points in the tiered system—that fundamentally improved upon prior cybersecurity systems and methods. *See* Compl. ¶¶ 37-38.

The benefits of the inventions are far reaching and go beyond the mere detection of previously unknown threats. For example, dependent claims 8, 12, 14, 25, 33, 37, and 39 of the '237 Patent and 8, 12, 14, 18, 19, and 22 of the '641 Patent require information from various probes to be correlated and used to improve the security of the overall system, whereas conventional

security systems were constrained to pattern matching at a single point in the network and lacked this functionality. *See also id.* It is the architecture claimed in the independent claims that enables the probes to correlate across probes in the dependent claims. *See id*. ¶ 38. This correlation of information across probes confers significant benefits to vendors like PAN because it allows detection of a new threat from one customer's status data to update the probes for all customers, thereby preventing that same threat from infiltrating all customers and enhancing the managed services PAN is able to offer. *See* '237 Patent, Claim 14 (reciting "cross-probe correlation"); *see also id.* 1:49-52 (disclosing the use of the invention to enable a managed service offering).

B. The Cybersecurity Industry, Including PAN, Has Broadly Adopted the Claimed Inventions and Touted Their Advantages.

Two decades after the filing of the Patents, PAN prominently features the benefits of the claimed architecture of the Patents despite arguing that such architectural features are abstract and not "specific technological improvement to computer functionality." Mot. at 10.

- Regarding the claimed architecture's ability to dynamically detect new unknown threats and improve the security of the system (Compl. ¶¶ 37-38), PAN warns that "[m]odern malware . . . constantly evolve[s] in order to avoid detection" and touts how its Strata security platform can "identify new types of threats." *See* Ex. 4, Network Security Overview at 5, 9; *see also id.* at 12 (touting how its "Next-Generation Firewalls . . . proactively stop unknown threats, gain network-wide visibility . . . , and reduce errors.").[8]

- Regarding the claimed architecture's analysis of residual status data (Compl. ¶ 37), PAN touts this feature for its WildFire product. *See* Compl. ¶¶ 54, 56.

- Regarding the claimed architecture's cross-probe correlation, *e.g.*, '237 Patent, Claim 14, PAN actively markets *WildFire*'s ability to "correlat[e] . . . threat data . . . [as] key to identifying and blocking ongoing intrusion attempts and future attacks . . . without requiring policy updates and configuration commits." *See* Ex. 4 at 38.

- Regarding the claimed architecture's ability to scale without sacrificing performance by allowing more probes to be added without overloading the entire system (*see, e.g.,* '641 Patent

[8] Ex. 4 is cited throughout the Complaint. *See*, *e.g.*, Compl. ¶¶ 45-46, 74-75, 78. The Court may consider such "documents 'integral to or explicitly referred to in the complaint'" on a motion to dismiss. *Doe v. Princeton Univ.*, 790 F. App'x 379, 382 n.2 (3d Cir. 2019) (citation omitted).

at 3:22-26), PAN's marketing materials publicize the importance of this inventive concept. *See, e.g.,* Ex. 4 at 11 ("The expanding perimeter and demands on network security have increased the need for multiple integrated security features that scale, don't affect network performance, and have the ability to protect against multiple threats in real time.").

IV. ARGUMENT

Patent eligibility is a question of law based on underlying factual findings. *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166 (Fed. Cir. 2018). Courts evaluate eligibility under the two-step framework of *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014). First, the Court "determine[s] whether the claims at issue are directed to a patent-ineligible concept such as an abstract idea." *SRI*, 930 F.3d at 1303 (citing *Alice,* 573 U.S. at 217). Second, if the claims are directed to an abstract idea, the Court must "consider the elements of each claim both individually and as an ordered combination to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 217 (internal quotations and citation omitted).

A. PAN's Motion Improperly Rests on Disputing Material Facts.

PAN repeatedly disputes well-pleaded factual allegations recited the Complaint, which is grounds alone for denying PAN's Motion. Indeed, "patent eligibility may be resolved at the Rule 12 stage only if there are no plausible factual disputes after drawing all reasonable inferences from the intrinsic and Rule 12 record in favor of the non-movant." *Coop.*, 50 F.4th at 130 (collecting cases); *see also S.I.SV.EL. Societa Italiana per lo Sviluppo Dell'Elettronica S.P.A v. Rhapsody Int'l Inc*., No. 18-cv-69, 2019 WL 2298795, at *6 (D. Del. May 30, 2019) (Burke, Mag. J.) ("material dispute of fact as to the conventionality of the ordered combination" was "in and of itself . . . sufficient to suggest that denial . . . [was] appropriate.").

PAN acknowledges that its arguments are based on disputing BT's factual allegations. Indeed, the entirety of Section IV.B of PAN's brief, entitled "The Claims Are Not Directed to an

Improvement in Computer Functionality" is dedicated to disputing BT's allegations about the improvements the Patents' claims bring to computer networks. To the extent there is a factual dispute about whether the Patents actually improved conventional computer security systems – which there clearly is – the Court must draw all reasonable inferences in favor of BT and deny PAN's Motion. *Coop.*, 50 F.4th at 130 (collecting cases); *see also MAZ Encryption Techs. LLC v. Blackberry Corp.,* No. 13-cv-304, 2016 WL 5661981, at *5 (D. Del. Sept. 29, 2016) (Burke, Mag. J.) ("the Court must take the specification's statements about the purported invention to be true."); *Genedics, LLC v. Meta Co.*, No. 17-cv-1062, 2018 WL 3991474, at *15 (D. Del. Aug. 21, 2018) (noting at "Rule 12(b)(6) stage, only plausibility is required.").

PAN argues that BT's "allegations are unsupported," are "contradicted by the specification," or "fail to demonstrate a specific technological improvement to computer functionality." Mot. at 10. But BT's allegations are based on the intrinsic record, including the patents, file histories, and the IPRs. *See*, *e.g.*, Compl. ¶¶ 16, 34 (citing Schneier Declaration from IPR), 38 (citing Notice of Allowability); *see also supra* III.A.[9]

PAN also argues that "a human can take steps *similar to* those recited in the claim." Mot. at 11 (emphasis added). But the Federal Circuit has held that "the human mind is not equipped to detect suspicious activity" in computer networks in the way that cybersecurity technology—like that claimed in the Patents—can. *SRI*, 930 F.3d at 1304 (rejecting argument that cybersecurity-related claims could "encompass steps that people can 'go through in their minds.'").

[9] Additional benefits related to "human resource problem[s]"—which PAN attempts to highlight from the background—do not prevent the claimed architecture from being an improvement to computer network technology. *Cf.* Mot. at 11; *see also WSOU Invs., LLC v. Netgear, Inc.*, No. 21-cv-1119, 2022 WL 2753005, at *2 (D. Del. July 14, 2022) (Burke, Mag. J.) (noting that one might conclude that a claim is directed to a broad concept if "look[ing] only to the patent's title or . . . the Background section."), *report and recommendation adopted*, No. 21-cv-1119, 2022 WL 3017109 (D. Del. July 29, 2022).

Critically, PAN ignores the inventiveness of the overall claimed architecture and breaks it into pieces, focusing instead on individual components that the Patents did not purport to invent. *See, e.g.*, Mot. at 13.[10] Improving computer networks is often reliant on architecture as opposed to any single feature. So even if the specification described the use of certain generic computer hardware to perform the claimed inventions, PAN's argument *still* fails because it cannot contest that the ordered combination of the claimed architecture is a useful improvement to computer networks. *See Coop.*, 50 F.4th at 135 ("[U]seful improvements to computer networks are patentable regardless of whether the network is comprised of standard computing equipment.").[11]

B. The Claims are Not Directed to An Abstract Idea; They Are Directed to Improvements in Computer Functionality By Way of a Novel Architecture.

At step one of the *Alice* analysis, the "court's task is [] not to determine whether claims merely involve an abstract idea at some level, but rather to examine the claims in their entirety to

[10] PAN disputes the factual allegation in Compl. ¶ 38 about "various probes" as somehow inconsistent with "the claim recit[ing] 'at least ***one*** probe.'" Mot. at 13 (emphasis in original). Not only is "at least one probe" consistent with multiple probes but Claims 14 and 39 of the '237 Patent and Claim 14 of the '641 Patent, expressly recite "cross-probe correlation," necessarily requiring multiple probes. In any event, PAN's argument regarding claim scope and construction is yet another example of a factual dispute that necessitates rejecting its motion at the Rule 12 stage.

[11] *See also Bascom Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016) ("The inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art . . . . [A]n inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces."); *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927 F.3d 1306, 1318 (Fed. Cir. 2019) ("But even assuming that Bluetooth was conventional at the time of these inventions, implementing a well-known technique with particular devices in a specific combination, like the two-device structure here, can be inventive."); *RICPI Commc'ns LLC v. JPS Interoperability Sols., Inc.*, No. 18-cv-1507, 2019 WL 1244077, at *5 (D. Del. Mar. 18, 2019) ("While the specification clearly concedes that the individual claim elements are themselves conventional, the arrangement of the claim elements is not."); *F45 Training Pty Ltd. v. Body Fit Training USA Inc.*, No. 20-cv-1194, 2021 WL 2779130, at *4 (D. Del. July 2, 2021) (recognizing it was "undisputed that the invention only use[d] generic computer components" but finding "dispute as to whether the combination of elements, including use of the generic computer components, is well understood, routine, and conventional as of the date of the invention.").

ascertain whether their character as a whole is directed to excluded subject matter." *Twilio, Inc. v. Telesign Corp.*, 249 F. Supp. 3d 1123, 1139 (N.D. Cal. 2017) (internal quotations and citations omitted). The Patents establish that the focus of the claimed advance over the prior art is a specific architecture for detecting and responding to new and constantly evolving attacks on computer networks. *See* Compl. ¶ 38. The Patents' claims are thus "necessarily rooted in computer technology in order to solve a specific problem in the realm of computer networks," and accordingly are not directed to an abstract idea at *Alice* step one. *SRI*, 930 F.3d at 1303.

PAN's argument that the Patents are directed to "collecting, filtering, analyzing, and transmitting data, and then making modifications based on feedback . . . [using] a generic computer network operating in its normal, expected manner," Mot. at 8, not only oversimplifies the claims, but also mischaracterizes their "character as a whole." *Affinity Labs of Tex., LLC v. DIRECTV, LLC,* 838 F.3d 1253, 1257 (Fed. Cir. 2016) (citation omitted).[12] The Patent claims recite a specific architecture for improving prior art computer network security that "spawned an entirely new product category" and fundamentally transformed the field of cybersecurity. Compl. ¶¶ 29, 34-37.

The Patent claims are strikingly similar to those in *SRI*, 930 F.3d 1295, which the Federal Circuit held were not abstract under *Alice* step one. In *SRI,* the Court found the claims directed to advancements in the field of cybersecurity. *Id.* at 1303. Particularly, the Court found them "directed to using a specific technique" (namely, "a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors") to "solve a

[12] PAN's generalization of the claims as directed to mere "data" also conflicts with Judge Connolly's construction of "status data." Ex. 3 at 1 ("data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components."). PAN's dispute over the proper scope of the Patent claims is yet another reason to deny its motion at this stage. *See Aatrix Software, Inc. v. Green Shades Software, Inc.,* 882 F.3d 1121, 1125 (Fed. Cir. 2018).

technological problem arising in computer networks: identifying hackers or potential intruders into the network." *Id.* In doing so, the Federal Circuit rejected an argument nearly identical to PAN's. *Compare, e.g.,* Mot. at 7-8 (arguing that claims are directed to "collecting, filtering, analyzing, and transmitting data, and . . . generic computing components"), *with SRI*, 930 F.3d at 1303-04 (rejecting argument that claims were "directed to just analyzing data from multiple sources to detect suspicious activity" and did not involve an "improvement to computer functionality itself.") (citation omitted).

Here, as in *SRI*, the "'focus of the claims is on the specific asserted improvement in computer capabilities'—that is, providing a network defense system that monitors network traffic in real-time to automatically detect large-scale attacks." *SRI*, 930 F.3d at 1303 (quoting *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335-36 (Fed. Cir. 2016)). Indeed, the Patents similarly "improve[] the technical functioning of the computer and computer networks by reciting a specific technique for improving computer network security." *Id.* at 1303-04 (finding based on specification that the "claimed invention [was] directed to solving [prior art] weaknesses in conventional networks and provide[d] 'a framework for the recognition of more global threats.'"); *see also TecSec, Inc. v. Adobe Inc.,* 978 F.3d 1278, 1295 (Fed. Cir. 2020) (finding claims directed at "solving a problem specific to computer data networks" where the "combination of labeling with the required encryption" was not abstract); *CardioNet, LLC v. InfoBionic, Inc*., 955 F.3d 1358, 1371 (Fed. Cir. 2020) (finding generalization of "asserted claims as being directed to collecting, analyzing, and reporting data [was] inconsistent with [] instruction that courts 'be careful to avoid oversimplifying the claims' by looking at them generally and failing to account for the specific requirements of the claims.") (citation omitted); *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1348 (Fed. Cir. 2018), *as amended* (Nov. 20, 2018) ("Improving security . . . can be a non-

abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem."); *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1349 (Fed. Cir. 2017) (holding claims that specified a "particular configuration of [] sensors and a particular method of using the raw data from the sensors" was not abstract); *Gracenote, Inc. v. Free Stream Media Corp.*, No. 18-cv-1608, 2019 WL 6728450, at *3 (D. Del. Dec. 11, 2019) (finding known elements in an "*unconventional* manner to *improve* [] accuracy" was improving computer technology itself (emphasis in original)).

The decisions finding abstractness that PAN relies on analyzed claims implementing human activity with a computer – not the type of architecture the Patents claim. *See IBM Corp. v. Zillow Grp., Inc.*, 50 F.4th 1371, 1378 (Fed. Cir. 2022) (claims "directed to limiting and coordinating the display of information based on a user selection."); *Content Extraction & Transmission LLC v. Wells Fargo Bank Nat'l Ass'n*, 776 F.3d 1343, 1348 (Fed. Cir. 2014) (claims that merely used computer and digital scanner to collect, recognize, and store data); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016) (claims merely "collecting information, analyzing it, and displaying certain results" in the context of an electric power grid); *Bascom Glob. Internet Servs., Inc.*, 827 F.3d at 1348 (claims directed to "content filtering system for filtering content") (citation omitted); *SAP Am., Inc.*, 898 F.3d at 1164 (method for "calculating, analyzing and displaying investment data.").[13]

[13] PAN also cites several cases in support of its argument that "optimizing a system using feedback is an abstract idea." Mot. at 9. Although those cases may use the word "feedback" or tangentially relate to optimizing, they do not actually discuss whether optimizing a system using feedback is abstract. *See In re Rosenberg*, 813 F. App'x 594, 596 (Fed. Cir. 2020) (finding that "*deciding whether to* fine-tune a given system" was abstract (emphasis added)); *Twilio,* 249 F. Supp. 3d at 1144 (finding that "*[s]electing the best option* based on separately-received feedback [was] a fundamental activity . . . long [] performed by humans." (emphasis added)); *ICON Health & Fitness, Inc. v. Polar Electro Oy*, 243 F. Supp. 3d 1229, 1238-39 (D. Utah 2017) (finding as abstract *a method for providing feedback*, which focused on gathering and aggregating data), *aff'd*,

Because the claims of the Patents are not directed to an abstract idea, the Court need not reach *Alice* step two. PAN's Motion should be denied at *Alice* step one.

C. The Claims Contain Inventive Concepts Sufficient to Transform any Alleged Abstract Idea into Patent Eligible Subject Matter.

A court should reach step two of the *Alice* framework only if the claims are directed to ineligible subject matter. *SRI*, 930 F.3d at 1304. If the Court reaches *Alice* step two, which it need not here, it should deny PAN's Motion because BT's complaint (at minimum) plausibly alleges that the claims "contain[] several alleged inventive concepts . . . compared to the prior art." *Coop.*, 50 F.4th at 131. Based upon the facts alleged in BT's Complaint, PAN simply cannot meet its burden to establish that the claims of the Patents were "well-understood, routine and conventional to a skilled artisan in the relevant field" upon "clear and convincing evidence." *TMI Sols. LLC v. Bath & Body Works Direct, Inc.*, No. 17-cv-965, 2018 WL 4660370, at *4 (D. Del. Sept. 28, 2018) (quoting *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018)).

Indeed, PAN's factual errors about the nature and scope of the claims and the improvements to the cybersecurity field, described in *supra* Section IV.A, are alone grounds to find that PAN has not shown that the claims are merely well-understood, routine and conventional to a skilled artisan in the relevant field—particularly because the Court must draw all reasonable inferences in favor of BT. *Coop.*, 50 F.4th at 130 (collecting cases).

As the Complaint explains, the claims of the Patents disclose a novel "architecture for unearthing and addressing network intrusions . . . now [] widely adopted throughout the cybersecurity industry, including by PAN." Compl. ¶ 29; *supra* Section I. The Patents "take an

717 F. App'x 1005 (Fed. Cir. 2018). Moreover, even if optimizing a system using feedback was abstract, that idea would not "meaningfully capture[] the 'character as a whole'" of the claims of the Patents. *Cf. Twilio*, 249 F. Supp. 3d at 1143.

approach that differs greatly from the conventional approach." Compl. ¶ 37. The claims are a marked improvement over prior art cybersecurity methods, which "focused on prevention as opposed to monitoring, detection, and response." *Id.* ¶ 36. These well-pleaded facts show that "the elements of each claim both individually and 'as an ordered combination' . . . 'transform the nature of the claim' into a patent-eligible application" and "ensure[s] that the claim amounts to 'significantly more' than the [alleged] abstract idea itself." *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1303 (Fed. Cir. 2018) (quoting *Alice*, 573 U.S. at 217).

PAN argues that individual elements within the claims of the Patents are "generic" and thus "cannot supply an inventive concept." Mot. at 15-20. Again, PAN misses the point. Even assuming PAN is correct in its assertion that the individual elements are standard components "[U]seful improvements to computer networks are patentable *regardless of whether the network is comprised of standard computing equipment*." *Coop.*, 50 F.4th at 135 (emphasis added). Conspicuously absent from PAN's brief is any argument contradicting that the claims in the Patents were a marked improvement of the detection of cybersecurity threats over prior conventional methods. *C.f. Affinity Labs*, 838 F.3d at 1257. Nor could it—given that PAN's marketing materials prominently advertise the benefits of the architecture claimed in the Patents. *See supra* Section III.B.

V. CONCLUSION

BT respectfully requests that the Court deny PAN's Motion.

POTTER ANDERSON & CORROON LLP

By: */s/ Philip A. Rovner*
Philip A. Rovner (#3215)
Jonathan A. Choa (#5319)
Hercules Plaza
P.O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com
jchoa@potteranderson.com

Attorneys for Plaintiff
British Telecommunications plc
and BT Americas, Inc.

OF COUNSEL:

Bart H. Williams
PROSKAUER ROSE LLP
2029 Century Park East
Suite 2400
Los Angeles, California 90067
310-557-2900
bwilliams@proskauer.com

Baldassare Vinti
Nolan M. Goldberg
PROSKAUER ROSE LLP
Eleven Times Square
New York, New York 10036
212-969-3000
bvinti@proskauer.com
ngoldberg@proskauer.com

Edward Wang
PROSKAUER ROSE LLP
1001 Pennsylvania Avenue NW
Suite 600
Washington, DC 20004
202-416-6800
ewang@proskauer.com

Dated: March 20, 2023
10695808